

A New Family of Generalized 3D Cat Maps ¹

Yue Wu, *Student Member, IEEE*, Sos Agaian, *Senior Member, IEEE*,
and Joseph P. Noonan, *Life Member, IEEE*,

Abstract

Since the 1990s chaotic cat maps are widely used in data encryption, for their very complicated dynamics within a simple model and desired characteristics related to requirements of cryptography. The number of cat map parameters and the map period length after discretization are two major concerns in many applications for security reasons. In this paper, we propose a new family of 36 distinctive 3D cat maps with different spatial configurations taking existing 3D cat maps [1]–[4] as special cases. Our analysis and comparisons show that this new 3D cat maps family has more independent map parameters and much longer averaged period lengths than existing 3D cat maps. The presented cat map family can be extended to higher dimensional cases.

Index Terms

Arnold Transform, Image Encryption, Cat Map, Automorphism

I. INTRODUCTION

In the last decade, many efforts have been recognized to study behaviors of dynamic systems and related applications. As one type of dynamic systems with very complicated behaviors, chaos systems are widely reported in mathematics, physics, engineering, economics, and biology. Especially for cryptography and encryption, chaotic cryptosystems [5] are demonstrated to have many analogous to conventional encryption methods [2], *e.g.* a conventional algorithm is sensitive to keys, while a chaotic system is sensitive to its initial values and parameters. Chaotic encryption systems also provide better solutions for image encryption where the conventional method are not suitable due to many intrinsic features of

Yue Wu and Joseph P. Noonan is with the Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155, United States; e-mail: ywu03@ece.tufts.edu.

Sos Agaian is with the Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, United States.

images [2], *e.g.* bulk data nature and high correlations between pixels. Consequently, numerous chaotic encryption algorithms have been proposed in literature based on various principles [2], [6]–[8]. Among these applications, Arnold’s cat map and its variants are commonly employed as a fundamental building block for data encryption [1]–[4], [7], [9]–[11], watermarking [12], and pattern recognition [13].

Arnold’s cat map [2], [14] is a discrete chaotic map named after *Vladimir Arnold*. Specifically, it is ergodic and mixing, a C-system, a K-system and a Bernoulli system [14]. Mathematically, Arnold’s cat map is defined in Eq. (1)

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \mathbf{C} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \quad (1)$$

where the transform matrix \mathbf{C} is defined as

$$\mathbf{C} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \quad (2)$$

In order to achieve higher map randomness and thus a more secure cryptosystem, the cat matrix \mathbf{C} of Arnold’s cat map is commonly replaced by Eq. (3), where new parameters help increase key spaces to resist brute-force attacks and longer averaged period lengths help improve map randomness to resist statistical attacks.

$$\mathbf{C}_{para}^{2D} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \quad (3)$$

Based on Eq. (3), many efforts [1]–[4] are put on designing 3D cat maps to further increase the parameter space and map randomness. However, we notice that 1) they failed to consider all possible spatial configurations of a 3D cat map; and 2) their 3D cat map matrix elements are designed in more correlate rather than independent to each other.

In this paper, we propose a new family of 3D cat maps with improvements on existing 3D cat maps [1]–[4]. This new family contains more parameters with longer averaged period lengths and taking these commonly used 3D cat maps as special cases. The rest of the paper is organized as follows: Section II reviews four existing 3D cat maps; Section III introduces our algorithm for generating the new 3D cat map family; Section IV analyzes the averaged period lengths of the proposed 3D cat maps with other 3D cat maps; and Section V concludes the letter.

II. EXISTING 3D CAT MAPS

Based on the parametric 2D cat map in Eq. (3), Lian *et al.* [1] proposed a parametric 3D cat map \mathbf{C}_L^{3D} in 2003 by extending 2D cat map in zx plane and yz plane.

$$\mathbf{C}_L^{3D} = \begin{bmatrix} 1 & 0 & a \\ bc & 1 & abc + c \\ bcd + b & d & abcd + ab + cd + 1 \end{bmatrix} \quad (4)$$

Later on, in 2004 Chen *et al.* [2] proposed a family of parametric 3D cat maps defined in Eq. (5) by composing three fundamental parametric 3D cat maps on xy and yz and zx planes defined in Eqs. (6), (7) and (8), respectively.

$$\mathbf{C}_C^{3D} = \mathbf{C}_C^{xy} \mathbf{C}_C^{yz} \mathbf{C}_C^{zx} \quad (5)$$

$$\mathbf{C}_C^{xy} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a_x \\ 0 & b_x & a_x b_x + 1 \end{bmatrix} \quad (6)$$

$$\mathbf{C}_C^{yz} = \begin{bmatrix} 1 & 0 & a_y \\ 0 & 1 & 0 \\ b_y & 0 & a_y b_y + 1 \end{bmatrix} \quad (7)$$

$$\mathbf{C}_C^{zx} = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (8)$$

Based on Chen's cat map, Liu *et al.* [3] proposed an improved 3D cat map \mathbf{C}_U^{3D} in 2008 by introducing new parameters c and d as shown in Eq. (9)

$$\mathbf{C}_U^{3D} = \begin{bmatrix} 1 & a & 0 \\ b & ab + 1 & 0 \\ c & d & 1 \end{bmatrix} \quad (9)$$

Recently in [4], Pan *et al.* introduced their 3D cat map \mathbf{C}_P^{3D} based on Chen's method, but in a different

formulation from Liu *et al.* 's.

$$\mathbf{C}_P^{3D} = \begin{bmatrix} 1 & a & c \\ b & ab+1 & bc \\ d & abcd & cd+1 \end{bmatrix} \quad (10)$$

It is worthwhile note that all these cat maps satisfy the condition that the determinant of 3D cat matrix is 1, *i.e.*

$$|\mathbf{C}_L^{3D}| = |\mathbf{C}_C^{3D}| = |\mathbf{C}_U^{3D}| = |\mathbf{C}_P^{3D}| = 1$$

III. A NEW FAMILY OF 3D CAT MAPS

One common feature of existing 3D cat maps [1]–[4] that they are all extended from the 2D cat map \mathbf{C}_{para}^{2D} defined in Eq. (3), which is indeed a general form of 2D cat but only one out of four possible spatial configurations as shown in Eqs. (11)–(14):

$$\mathbf{C}_1^{2D} = \mathbf{C}_{para}^{2D} \quad (11)$$

$$\mathbf{C}_2^{2D} = \begin{bmatrix} a & 1 \\ ab-1 & b \end{bmatrix} \quad (12)$$

$$\mathbf{C}_3^{2D} = \begin{bmatrix} a & ab-1 \\ 1 & b \end{bmatrix} \quad (13)$$

$$\mathbf{C}_4^{2D} = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix} \quad (14)$$

As can be seen, these configurations are inequivalent to each other in general because none of them has the unitary element located in the same position. However, spatial configurations are fail to be considered in previous 3D cat maps [1]–[4].

Meanwhile, we also notice that constructing 3D cat maps by directly extending the 2D cat map \mathbf{C}_{para}^{2D} as done in [1]–[4] is not necessary, because all what we need is to construct a 3×3 matrix \mathbf{C}^{3D} with the constraint that its determinant is 1 [2]. In other words, we are looking for a 3×3 matrix \mathbf{C}_W^{3D} with the symbol set $\mathfrak{S} = \{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \mathfrak{e}, \mathfrak{f}, \mathfrak{g}, \mathfrak{h}, \mathfrak{i}\}$ as shown in Eq. (15) whose determinant satisfies Eq. (16).

$$\mathbf{C}_W^{3D} = \begin{bmatrix} \mathfrak{a} & \mathfrak{b} & \mathfrak{c} \\ \mathfrak{d} & \mathfrak{e} & \mathfrak{f} \\ \mathfrak{g} & \mathfrak{h} & \mathfrak{i} \end{bmatrix} \quad (15)$$

$$|\mathbf{C}_W^{3D}| = \mathfrak{a}\mathfrak{e}\mathfrak{i} + \mathfrak{b}\mathfrak{f}\mathfrak{g} + \mathfrak{c}\mathfrak{d}\mathfrak{h} - \mathfrak{c}\mathfrak{e}\mathfrak{g} - \mathfrak{b}\mathfrak{d}\mathfrak{i} - \mathfrak{a}\mathfrak{f}\mathfrak{h} = 1 \quad (16)$$

We describe a general solution to the above constraint problem in Algorithm 1. This algorithm is able to generate 36 spatial configurations specified by parameter u and m for 3D cat maps, each configuration with six other independent parameters controlling cat matrix elements.

Algorithm 1. Cat Matrix $\mathbf{C}_{W_{um}}^{3D}$ Generator

Require: u is an integer in $\{1, 2, \dots, 9\}$

Require: m is an integer in $\{1, 2, 3, 4\}$

Ensure: $\mathbf{C}_{W_{um}}^{3D}$ is a 3D Cat matrix with $|\mathbf{C}_{W_{um}}^{3D}| = 1$

1. Set symbol \mathfrak{S}_u to 1 and compute the target determinant $\mathfrak{a}\mathfrak{e}\mathfrak{i} + \mathfrak{b}\mathfrak{f}\mathfrak{g} + \mathfrak{c}\mathfrak{d}\mathfrak{h} - \mathfrak{c}\mathfrak{e}\mathfrak{g} - \mathfrak{b}\mathfrak{d}\mathfrak{i} - \mathfrak{a}\mathfrak{f}\mathfrak{h} = 1$ by substituting $\mathfrak{S}_u = 1$
 2. Form the four symbols in the positive or negative diagonal containing the unitary symbol \mathfrak{S}_u to set \mathfrak{F}
 3. Collect the terms containing the symbol \mathfrak{F}_m on the left side of the equation and leave all the other terms on the right side with a name *rightside*
 4. Set the coefficient term of symbol \mathfrak{F}_m to 1 and result in symbol $\mathfrak{F}_m = \text{rightside}$.
 5. Output $\mathbf{C}_{W_{um}}^{3D}$ as a 3D cat map.
-

Details of why this algorithm works are illustrated by the following example. Assume $u = m = 1$, then we first set the unitary symbol $\mathfrak{S}_u = \mathfrak{S}_1 = \mathfrak{a} = 1$, *i.e.* we have

$$\mathbf{C}_{W_{11}}^{3D} = \begin{bmatrix} 1 & \mathfrak{b} & \mathfrak{c} \\ \mathfrak{d} & \mathfrak{e} & \mathfrak{f} \\ \mathfrak{g} & \mathfrak{h} & \mathfrak{i} \end{bmatrix}$$

. Consequently, the target determinant equation $|\mathbf{C}_{W_{11}}^{3D}| = 1$ become

$$\mathfrak{e}\mathfrak{i} + \mathfrak{b}\mathfrak{f}\mathfrak{g} + \mathfrak{c}\mathfrak{d}\mathfrak{h} - \mathfrak{c}\mathfrak{e}\mathfrak{g} - \mathfrak{b}\mathfrak{d}\mathfrak{i} - \mathfrak{f}\mathfrak{h} = 1$$

We then obtain a symbol set $\mathfrak{F} = \{\mathfrak{e}, \mathfrak{i}, \mathfrak{f}, \mathfrak{h}\}$ for those either along the positive or the negative diagonal containing the symbol \mathfrak{S}_1 ; and collect all terms containing symbol $\mathfrak{F}_m = \mathfrak{F}_1 = \mathfrak{e}$ on the left side of the equation, leaving all the other terms on the right side, namely

$$(\mathfrak{i} - \mathfrak{c}\mathfrak{g})\mathfrak{e} = 1 - \mathfrak{b}\mathfrak{f}\mathfrak{g} - \mathfrak{c}\mathfrak{d}\mathfrak{h} + \mathfrak{b}\mathfrak{d}\mathfrak{i} + \mathfrak{f}\mathfrak{h}$$

Next we set the coefficient term of symbol \mathfrak{e} to 1, *i.e.* $\mathfrak{i} = \mathfrak{c}\mathfrak{g} + 1$, and the simplified equation implies that

$$\mathfrak{e} = 1 - \mathfrak{b}\mathfrak{f}\mathfrak{g} - \mathfrak{c}\mathfrak{d}\mathfrak{h} + \mathfrak{b}\mathfrak{d}(\mathfrak{c}\mathfrak{g} + 1) + \mathfrak{f}\mathfrak{h}$$

And we finish the 3D cat map construction, because $\mathbf{C}_{W_{11}}^{3D}$ in Eq. (17) is already of a 3×3 matrix with determinant 1.

$$\mathbf{C}_{W_{11}}^{3D} = \begin{bmatrix} 1 & \mathfrak{b} & \mathfrak{c} \\ \mathfrak{d} & \mathfrak{b}\mathfrak{d} + \mathfrak{f}\mathfrak{h} - \mathfrak{b}\mathfrak{f}\mathfrak{g} - \mathfrak{c}\mathfrak{d}\mathfrak{h} + \mathfrak{b}\mathfrak{c}\mathfrak{d}\mathfrak{g} + 1 & \mathfrak{f} \\ \mathfrak{g} & \mathfrak{h} & \mathfrak{c}\mathfrak{g} + 1 \end{bmatrix} \quad (17)$$

The other three variants with unitary element $a = 1$ of the 3D cat map family are shown below:

$$\mathbf{C}_{W_{12}}^{3D} = \begin{bmatrix} 1 & \mathfrak{b} & \mathfrak{c} \\ \mathfrak{d} & \mathfrak{b}\mathfrak{d} + 1 & \mathfrak{f} \\ \mathfrak{g} & \mathfrak{h} & \mathfrak{c}\mathfrak{g} + \mathfrak{f}\mathfrak{h} - \mathfrak{b}\mathfrak{f}\mathfrak{g} - \mathfrak{c}\mathfrak{d}\mathfrak{h} + \mathfrak{b}\mathfrak{c}\mathfrak{d}\mathfrak{g} + 1 \end{bmatrix} \quad (18)$$

$$\mathbf{C}_{W_{13}}^{3D} = \begin{bmatrix} 1 & \mathfrak{b} & \mathfrak{c} \\ \mathfrak{d} & \mathfrak{e} & \mathfrak{c}\mathfrak{d} + 1 \\ \mathfrak{g} & \mathfrak{b}\mathfrak{g} + \mathfrak{e}\mathfrak{i} - \mathfrak{c}\mathfrak{e}\mathfrak{g} - \mathfrak{b}\mathfrak{d}\mathfrak{i} + \mathfrak{b}\mathfrak{c}\mathfrak{d}\mathfrak{g} - 1 & \mathfrak{i} \end{bmatrix} \quad (19)$$

$$\mathbf{C}_{W_{14}}^{3D} = \begin{bmatrix} 1 & \mathfrak{b} & \mathfrak{c} \\ \mathfrak{d} & \mathfrak{e} & \mathfrak{c}\mathfrak{d} + \mathfrak{e}\mathfrak{i} - \mathfrak{c}\mathfrak{e}\mathfrak{g} - \mathfrak{b}\mathfrak{d}\mathfrak{i} + \mathfrak{b}\mathfrak{c}\mathfrak{d}\mathfrak{g} - 1 \\ \mathfrak{g} & \mathfrak{b}\mathfrak{g} + 1 & \mathfrak{i} \end{bmatrix} \quad (20)$$

In general, a symbolic 3D cat map of the possible 36 spatial configurations can be easily obtained in a similar manner by feeding different us and ms in Algorithm 1, each configuration contains six independent parameters like those in Eqs. (17)-(20). Therefore, each new parametric 3D cat map is associated with eight independent parameters, two controlling spatial configurations and six controlling matrix elements. Consequently, this new family of 3D cat maps have more parameters but less correlated matrix elements than existing 3D cat maps [1]–[4]. Detailed comparisons about parameters and matrix elements between different 3D cat maps are summarized in Table I.

TABLE I: Elements and Parameters in 3D Cat Maps

| Number of Items | Existing 3D Cat Maps | | | | |
|------------------------|----------------------|---------------------|---------------------|---------------------|---------------------|
| | \mathbf{C}_L^{3D} | \mathbf{C}_C^{3D} | \mathbf{C}_U^{3D} | \mathbf{C}_P^{3D} | \mathbf{C}_W^{3D} |
| Constant 0 Elements | 1 | 0 | 2 | 0 | 0 |
| Constant 1 Elements | 2 | 0 | 2 | 1 | 1 |
| 1 Parameter Elements | 2 | 2 | 4 | 4 | 6 |
| 2+ Parameter Elements | 4 | 7 | 1 | 4 | 2 |
| Parameters | 4 | 6 | 4 | 4 | 8 |
| Spatial Configurations | 1 | 1 | 1 | 1 | 36 |

It is worthwhile to note that the proposed 3D cat map family includes previous 3D cat maps [1]–[4] as special cases as shown in Table II, where each existing 3D cat map \mathbf{C}^{3D} can be denoted by $\mathbf{C}_{W_{um}}^{3D}$ with the eight parameters listed the table and symbol \star indicates either constant elements or dependent elements on two or more parameters. For example, \mathbf{C}_P^{3D} is a special case of $\mathbf{C}_{W_{um}}^{3D}$ because Eq. (21) holds.

$$\mathbf{C}_P^{3D} = \mathbf{C}_{W_{um}}^{3D} \big|_{\substack{u=1, m=2 \\ b=a, c=c, d=b, f=bc, g=d, h=abcd}} \quad (21)$$

For verification, simply substitute these parameter values in $\mathbf{C}_{W_{12}}^{3D}$. And we obtain \star elements $\mathbf{a} = 1$, $\mathbf{e} = b\mathbf{d} + 1 = ab + 1$, and $\mathbf{i} = c\mathbf{g} + f\mathbf{h} - b\mathbf{f}\mathbf{g} - c\mathbf{d}\mathbf{h} + b\mathbf{c}\mathbf{d}\mathbf{g} + 1 = cd + (bc)(abcd) - abcd - cb(abcd) + acbd + 1 = cd + 1$, which are indeed the three corresponding elements of \mathbf{C}_P^{3D} defined in Eq. (10).

TABLE II: Denoting existing 3D cat maps with $\mathbf{C}_{W_{um}}^{3D}$

| Para. | Existing 3D Cat Maps | | | | | |
|--------------|----------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| | \mathbf{C}_L^{3D} | \mathbf{C}_C^{xy} | \mathbf{C}_C^{yz} | \mathbf{C}_C^{zx} | \mathbf{C}_U^{3D} | \mathbf{C}_P^{3D} |
| u | 1 | 1 | 1 | 1 | 1 | 1 |
| m | 2 | 1 | 1 | 1 | 1 | 2 |
| \mathbf{a} | \star | \star | \star | \star | \star | \star |
| \mathbf{b} | 0 | 0 | 0 | a_z | a | a |
| \mathbf{c} | a | 0 | a_y | 0 | 0 | c |
| \mathbf{d} | bc | 0 | 0 | b_z | b | b |
| \mathbf{e} | \star | \star | \star | \star | \star | \star |
| \mathbf{f} | $abc + c$ | a_x | 0 | 0 | 0 | bc |
| \mathbf{g} | $bcd + b$ | 0 | b_y | 0 | c | d |
| \mathbf{h} | d | b_x | 0 | 0 | d | $abcd$ |
| \mathbf{i} | \star | \star | \star | \star | \star | \star |

Meanwhile, the new proposed 3D cat maps can be extended to a more general case simply by multiplying 3D cat maps with interested configurations. In general, we can construct such a mixed 3D cat map $\mathbf{C}_{W_s}^{3D}$ as shown in Eq. (22), where s_{um} is the indicator function for configuration (u, m) defined in Eq. (23). In this way, we are able to construct a more general 3D cat map with 36 new indicator parameters $\{s_{11}, s_{12}, s_{13}, s_{14}, s_{21}, \dots, s_{94}\}$.

$$\mathbf{C}_{W_s}^{3D} = \prod_{u=1}^9 \prod_{m=1}^4 (\mathbf{C}_{W_{um}}^{3D})^{s_{um}} \quad (22)$$

$$s_{um} = \begin{cases} 1, & \text{if } \mathbf{C}_{W_{um}}^{3D} \text{ is interested} \\ 0, & \text{otherwise} \end{cases} \quad (23)$$

IV. SIMULATION RESULTS

In many applications [2]–[4], a 3D cat map is used over a module N as a finite state system shown in Eq. (24), where the vector $[x_t, y_t, z_t]^T$ and $[x_{t+1}, y_{t+1}, z_{t+1}]^T$ denote the discrete spatial coordinates at the time t and $t + 1$, respectively.

$$\begin{bmatrix} x_{t+1} \\ y_{t+1} \\ z_{t+1} \end{bmatrix} = \mathbf{C}^{3D} \begin{bmatrix} x_t \\ y_t \\ z_t \end{bmatrix} \bmod N \quad (24)$$

The period length of this 3D cat map can be defined in Eq. (26), where \mathbf{I} is the 3×3 identity matrix.

$$P_N(\mathbf{C}^{3D}) = \arg \min_{t \in \mathbb{Z}^+} \left\{ (\mathbf{C}^{3D})^t \bmod N = \mathbf{I} \right\} \quad (25)$$

TABLE III: Averaged Period Lengths of 3D Cat Maps

| N | 3D Cat Maps | | | | | | |
|-----|---------------------|---------------------|---------------------|---------------------|----------------------------|----------------------------|----------------------------|
| | \mathbf{C}_L^{3D} | \mathbf{C}_C^{3D} | \mathbf{C}_U^{3D} | \mathbf{C}_P^{3D} | $\mathbf{C}_{W_{11}}^{3D}$ | $\mathbf{C}_{W_{12}}^{3D}$ | $\mathbf{C}_{W_{um}}^{3D}$ |
| 10 | 30.9 | 53.7 | 8.9 | 20.7 | 58.1 | 59.2 | 67.2 |
| 20 | 50.7 | 85.0 | 14.4 | 32.3 | 88.5 | 90.2 | 99.2 |
| 30 | 142.3 | 320.9 | 19.8 | 55.4 | 357.6 | 362.2 | 442.6 |
| 40 | 81.3 | 143.6 | 24.4 | 51.3 | 156.5 | 154.9 | 176.7 |
| 50 | 156.7 | 274.2 | 49.3 | 109.3 | 292.9 | 293.0 | 330.4 |
| 60 | 217.4 | 475.5 | 30.0 | 73.2 | 492.1 | 512.3 | 589.0 |
| 70 | 447.8 | 961.5 | 46.1 | 244.5 | 1045.7 | 1079.4 | 1228.3 |
| 80 | 155.3 | 276.1 | 47.3 | 92.2 | 300.1 | 301.2 | 330.4 |
| 90 | 315.2 | 673.0 | 46.8 | 111.8 | 764.8 | 762.1 | 929.5 |
| 100 | 247.3 | 420.3 | 77.0 | 164.9 | 439.3 | 439.4 | 505.7 |

Since any orbit in a finite state system is periodic, the system randomness can be largely reflected by averaged period length. And it is desired to have a 3D cat map with longer period lengths [15]. In regarding to the randomness of 3D cat maps, we perform the following comparisons on averaged period lengths using computer simulations. Specifically, we test six 3D cat maps \mathbf{C}_L^{3D} , \mathbf{C}_C^{3D} , \mathbf{C}_U^{3D} , \mathbf{C}_P^{3D} , $\mathbf{C}_{W_{11}}^{3D}$, $\mathbf{C}_{W_{12}}^{3D}$ and $\mathbf{C}_{W_{um}}^{3D}$, and measure the period length of each cat map with a random set of parameters. Repeat this experiment 10,000 times and calculate the averaged period length for a 3D cat map under the module N denoted as $\overline{P_N(\mathbf{C}^{3D})}$ defined in Eq. (26).

$$\overline{P_N(\mathbf{C}^{3D})} = \sum_{j=1}^{10000} P_N(\mathbf{C}_j^{3D}) \quad (26)$$

where C_j^{3D} is the j th randomly generated C^{3D} matrix. Simulation results of these averaged period lengths for $N = \{10, 20, \dots, 100\}$ are given in Table III. These results clearly indicate that the new proposed 3D cat maps $C_{W_{11}}^{3D}$, $C_{W_{12}}^{3D}$, and $C_{W_{um}}^{3D}$ have much longer averaged period lengths than cat maps [1]–[4].

V. CONCLUSION

In this letter, we have proposed a new family of 3D cat maps with eight parameters, two parameters controlling the cat map spatial configuration and the other six controlling the cat matrix elements. It incorporates the conventional 3D cat maps proposed by Lian *et al.* [1], Chen *et al.* [2], Liu *et al.* [3] and Pan *et al.* [4] as special cases. It also outperforms these maps by providing more independent parameters and longer averaged period lengths. Both improvements on 3D cat maps are very meaningful for enhancing the security of chaotic cryptosystems and image encryption algorithms [1]–[4], [7], [9]–[11]. A 3D cat map based system using new proposed 3D cat maps will have a larger key space to resist brute-force attacks and a longer averaged period length to resist statistical attacks. The presented framework is "universal" and allows extending to higher dimensional cat maps [8], [16].

REFERENCES

- [1] S. Lian, Y. Mao, and Z. Wang, "3d extensions of some 2d chaotic maps and their usage in data encryption," in *4th International Conference on Control and Automation*, june 2003, pp. 819–823.
- [2] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761.
- [3] H. Liu, Z. Zhu, H. Jiang, and B. Wang, "A novel image encryption algorithm based on improved 3d chaotic cat map," in *The 9th International Conference for Young Computer Scientists*. IEEE, 2008, pp. 3016–3021.
- [4] T. Pan and D. Li, "A new algorithm of image encryption based on 3d arnold cat," in *Advanced Engineering Forum*, vol. 1. Trans Tech Publ, 2011, pp. 183–187.
- [5] J. Amigó, L. Kocarev, and J. Szczepanski, "Theory and practice of chaotic cryptography," *Physics Letters A*, vol. 366, no. 3, pp. 211–216, 2007.
- [6] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934.
- [7] A. Kumar and M. Ghose, "Substitution-diffusion based image cipher using chaotic standard map and 3d cat map," *Information Processing and Management*, pp. 34–38, 2010.
- [8] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons and Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.
- [9] C. Fu, B. bin Lin, Y. sheng Miao, X. Liu, and J. jie Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415 – 5423, 2011.
- [10] A. Kalso and M. Ghebleh, "A novel image encryption algorithm based on a 3d chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, 2011.

- [11] Z. Liu, M. Gong, Y. Dou, F. Liu, S. Lin, M. Ashfaq Ahmad, J. Dai, and S. Liu, "Double image encryption by using arnold transform and discrete fractional angular transform," *Optics and Lasers in Engineering*, 2011.
- [12] Q. chuan Zhong and Q. xin Zhu, "A dct domain color watermarking scheme based on chaos and multilayer arnold transformation," in *International Conference on Networking and Digital Society*, vol. 2, may 2009, pp. 209 –212.
- [13] X. Deng and D. Zhao, "Color component 3d arnold transform for polychromatic pattern recognition," *Optics Communications*, 2011.
- [14] J. Ford, G. Mantica, and G. Ristow, "The arnol'd cat: Failure of the correspondence principle," *Physica D: Nonlinear Phenomena*, vol. 50, no. 3, pp. 493–520, 1991.
- [15] N. Nagaraj, M. C. Shastri, and P. G. Vaidya, "Increasing average period lengths by switching of robust chaos maps in finite precision," *The European Physical Journal - Special Topics*, vol. 165, pp. 73–83, 2008.
- [16] Y. Liu, W. Tang, and H. Kwok, "Formulation and analysis of high-dimensional chaotic maps," in *IEEE International Symposium on Circuits and Systems*, may 2008, pp. 772 –775.